TRAINING AND AWARENESS FOR INFORMATION SECURITY AND PRIVACY   **5320**
(Revised 12/13)

Policy: Each state entity must establish and maintain an information security and privacy training and awareness program. State entity personnel must possess the knowledge and skills necessary to use information technology to the best advantage for the state. Each state entity must regularly assess the skills and knowledge of its personnel in relation to job requirements, identify and document training and professional development needs, and provide suitable training within the limits of available resources.

The training and awareness program shall ensure:

1. All personnel receive general security and privacy awareness training so that they understand the state entity information security policies, standards, procedures, and practices; and are knowledgeable about the various management, operational, and technical controls required to protect the information assets for which they are responsible.

2. Groups of personnel with special security training needs, such as application developers receive the necessary training.

3. Training records are maintained to support corrective action, audit and assessment processes.

4. The program content is maintained and evaluated for effectiveness on an ongoing basis.

State entity heads, Chief Information Officers (CIOs), ISOs, management, and information asset owners have key roles in information security training and awareness. The state entity head is responsible for ensuring an effective program is implemented state entity-wide. The scope and content of the awareness program must align with statewide policy, and with any state entity specific security needs and requirements.

Implementation Controls: NIST SP 800-53: Awareness and Training (AT)